PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04Q 7/38 | A3

(11) Internationale Veröffentlichungsnummer: **WO 00/14895**

(43) Internationales Veröffentlichungsdatum: 16. März 2000 (16.03.00)

(21) Internationales Aktenzeichen: PCT/DE99/02836

(22) Internationales Anmeldedatum: 7. September 1999 (07.09.99)

(30) Prioritätsdaten:
198 40 742.4 7. September 1998 (07.09.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Landgrabenweg 151, D–53227 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HAKE, Jens [DE/DE]; Südweg 4b, D–09240 Kemtau (DE). THELEN, Jörg [DE/DE]; Nesselroderstrasse 27, D–53227 Bonn (DE).

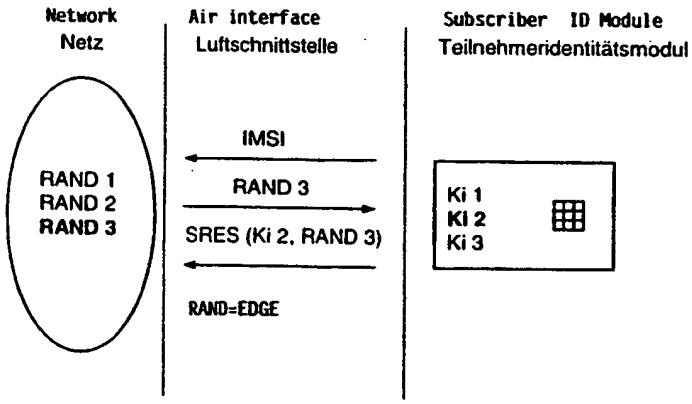
(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CZ, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 13. Juli 2000 (13.07.00)

(54) Title: METHOD FOR IMPROVING THE SECURITY OF AUTHENTICATION PROCEDURES IN DIGITAL MOBILE RADIO TELEPHONE SYSTEMS

(54) Bezeichnung: VERFAHREN ZUR ERHÖHUNG DER SICHERHEIT VON AUTHENTISIERUNGSVERFAHREN IN DIGITALEN MOBILFUNKSYSTEMEN



(57) Abstract

The invention relates to a method for improving the security of authentication procedures in digital mobile radio telephone systems. In order to make it more difficult if not impossible to work out a secret code KI, several different secret SIM–specific codes KI are contained in the mobile radio telephone network and on a subscriber identity module SIM and a code KI for the implementation of said authentication is selected from the various secret codes thus contained during the authentication process between the subscriber identity module and the mobile radio telephone system pertaining to said SIM.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Erhöhung der Sicherheit von Authentisierungsverfahren in digitalen Mobilfunksystemen. Um ein Ausspähen des geheimen Schlüssels KI zu erschweren, bzw. nahezu unmöglich zu machen, wird vorgeschlagen, dass im Mobilfunknetz und auf einem Teilnehmeridentitätsmodul mehrere verschieden geheime, SIM–spezifische Schlüssel KI vorgehalten werden, und bei der Authentisierung zwischen dem Teilnehmeridentitätsmodul und dem Mobilfunknetz von oder SIM aus den